

CLAIMS

We claim:

1. A method of operating an intrusion detection system, the method comprising the steps of:

taking a base action in response to detecting an intrusion;

updating an action counter in response to taking the base action;

comparing the value of the action counter to an action threshold;

updating an action variable when the value of the action counter meets the action

threshold;

checking a validity condition for satisfaction dependent upon the action variable; and

invoking a provision associated with the validity condition when the validity condition is

satisfied.

1 2. The method of claim 1, wherein the provision changes an element of a base intrusion set.

2 3. The method of claim 2, wherein the element of the base intrusion set is a signature event.

1 4. The method of claim 2, wherein the element of the base intrusion set is a signature event
2 counter.

5. The method of claim 2, wherein the element of the base intrusion set is a signature threshold.

6. The method of claim 2, wherein the element of the base intrusion set is a base action.

7. The method of claim 2, wherein the element of the base intrusion set is a weight.

1 8. The method of claim 1, wherein the provision changes an element of an action set.

1 9. The method of claim 8, wherein the element of the action set is an action counter.

- 1 10. The method of claim 8, wherein the element of the action set is an action threshold.
- 1 11. The method of claim 8, wherein the element of the action set is an action variable.
- 1 12. A method of operating an intrusion detection system, the method comprising the steps of:
- 2 detecting a signature event;
- 3 updating a signature event counter responsive to detecting the signature event;
- 4 comparing the value of the signature event counter to a signature threshold;
- 5 updating an action counter when the value of the signature event counter meets the
- 6 signature threshold;
- 7 comparing the value of the action counter to an action threshold;
- 8 updating an action variable when the value of the action counter meets the action
- 9 threshold;
- 10 checking a validity condition for satisfaction dependent upon the action variable; and

- 1 invoking a provision associated with the validity condition when the validity condition is
- 2 satisfied.

11/11/2020 11:11:11 AM

1 13. The method of claim 12, wherein the provision changes an element of a base intrusion set.

1 14. The method of claim 13, wherein the element of the base intrusion set is a signature event.

1 15. The method of claim 13, wherein the element of the base intrusion set is a signature event
counter.

1 16. The method of claim 13, wherein the element of the base intrusion set is a signature
threshold.

1 17. The method of claim 13, wherein the element of the base intrusion set is a base action.

1 18. The method of claim 13, wherein the element of the base intrusion set is a weight.

1 19. The method of claim 12, wherein the provision changes an element of an action set.

1 20. The method of claim 19, wherein the element of the action set is an action counter.

1 21. The method of claim 19, wherein the element of the action set is an action threshold.

1 22. The method of claim 19, wherein the element of the action set is an action variable.

Patent